ResearchGate

See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/358574416

Cloud Computing Service Provider Comparasion & Analysis | Komparasi & Analisis Penyedia Layanan Cloud Computing

Article · December 2021

CITATIONS
0

READS
45

4 authors, including:

Daffa Aslam
Bina Sarana Informatika
1 PUBLICATION **0** CITATIONS

SEE PROFILE

All content following this page was uploaded by Daffa Aslam on 13 February 2022.

The user has requested enhancement of the downloaded file.

Cloud Computing Service Provider

Comparasion & Analisis

Komparasi & Analisis Penyedia Layanan Cloud Computing

Daffa Aslam Multazam, Muggi Putra Pamungkas, Muhammad Fathur Rizky, Muhammad Alvan Fauzan

Data Science, Universitas Bina Sarana Informatika; Jl. Letnan Sutopo Bsd Serpong, Indonesia 15311

17191011@bsi.ac.id, 17190889@bsi.ac.id, 17191119@bsi.ac.id, 17191231@bsi.ac.id

Latar Belakang Masalah

Selain harga dan fungsionalitas, keamanan adalah salah satu aspek terpenting dari produk berbasis TI. Tidak hanya keamanan produk IT yang kuat terhadap serangan hacker, tetapi juga membutuhkan kepatuhan terhadap aturan dan kesepakatan antara pengguna dan penyedia saat memproses data pengguna. Merek mana yang menawarkan keamanan terbaik untuk ini? Penulis menjelaskan dan membandingkan merek utama penyedia komputasi awan. Oleh karena itu, platform tersebut telah mengetahui lisensi dan sertifikat audit yang dapat diakses pengguna dengan aman dan bebas (manajemen-ti.com). Selain itu, data yang diakses pengguna disimpan di server pusat yang disediakan oleh penyedia komputasi awan. Internet memasuki era baru, dan Internet, yang dimulai sebagai media informasi, telah berubah menjadi segalanya, dapat digunakan sebagai media komersial dan pendidikan, dan akan terus berkembang, sehingga diperlukan situs web dan server yang sangat dioptimalkan. Mendukung jumlah pengguna dan keamanan yang perlu Anda persiapkan jika terjadi sesuatu yang tidak terduga. Dilansir bahwa pengguna seluler telah mencapai 6,4 miliar dan akan terus bertambah sehingga diperlukan website dan server yang sudah sangat di optimalkan untuk menampung banyaknya user serta keamanan yang harus dipersiapkan bila terjadi hal yang tak di inginkan.(liputan6.com 2021)

Bagaimanapun, keamanan adalah bagian yang sangat penting dari komputasi awan itu sendiri, dengan banyak kasus pelanggaran data dari perusahaan besar, termasuk yang menginjak unicorn di Indonesia. Kejadian tersebut juga terjadi di pasar Tokopedia Indonesia pada bulan Mei lalu, menyebabkan pencurian data pengguna, membocorkan sekitar 91 juta data pengguna dari situs yang dijual, dan mengunduh data pengguna ke Internet secara gratis. Bahkan, kejadian ini terjadi pada tahun 2019 juga. Memang, untuk pelaku e-commerce seperti Lazada dan Bukalapak, pelakunya sendiri adalah warga Pakistan yang mencuri jutaan data pengguna e-commerce Indonesia. (cnnindonesia.com) Bahkan Global Cyber Security Index 2018 melakukan studi banding ke beberapa negara di kawasan Asia Tenggara dengan melihat skor eksposur dari minimal 0,4 hingga maksimal 0,6. Studi di Asia Tenggara secara khusus menargetkan Singapura, Malaysia, Thailand, Indonesia, dan Filipina. Indonesia sendiri di peringkat ke-4 jelas kalah dengan kompetitornya Singapura, Malaysia dan Thailand. Artinya, Indonesia masih rentan terhadap kejahatan keamanan siber dan mendapat peringkat terbaik (CNBC Indonesia 2020).

Beberapa perusahaan e-commerce di Indonesia melihat berbagai tanda kebocoran cyber. E-commerce di atas menggunakan setiap server perusahaan dengan kelemahan seperti biaya tinggi untuk menjaga server tetap berjalan, pemeliharaan , biaya operasi dari sudut pandang keamanan, dan tentu saja konsumsi daya yang tinggi. Jurnal ini menyajikan solusi khususnya dari sisi keamanan berupa perbandingan merek *cloud computing*. Dalam hal ini, tidak hanya menggambarkan seberapa kuat merek komputasi awan terhadap serangan peretasan, tetapi juga syarat dan ketentuan serta pedoman keamanan data dari masing-

masing perusahaan. Ambil salah satunya, Lazada, sebagai contoh. Mereka mendapatkan dari apa yang terjadi di tahun 2019 sendiri, dan Lazada termasuk salah satu e-commerce yang mengelola data dan menggunakan komputasi awan modern, yang diproses langsung oleh komputer itu sendiri. (CNBC Indonesia)

Pembahasan

AWS, Azure dan Google cloud adalah tiga penyedia cloud utama. Sementara *AWS* memiliki pangsa pasar yang lebih besar, Azure memiliki basis pelanggan yang lebih besar di antara perusahaan-perusahaan top Fortune. Sementara *AWS* memiliki keunggulan penggerak pertama, *Azure* mengejar dengan cepat. Dengan setiap pembaruan baru, mereka saling melacak, dan *Google Cloud* adalah produk layanan komputasi awan milik Google. Banyak yang membedakan tiga penyedia layanan cloud utama ini

Security Service Feature	***Aws***	***Azure***	***Google Cloud***
Identity and access management	*IAM*	*Active Directory*	*IAM*
Key management	*KMS*	*Key Vault*	*KMS*
Network	*VPC*	*Virtual Network, Express Route*	*VPC*
Security Check	*Trusted Advisor, AWS Inspector*	*Security Center*	*Cloud Security Posture Management (CSPM)*
Storage Security	*Data Encryption for S3*	*Storage Service Encryption (SSE)*	*Access Control Lists*
Monitoring	*CloudWatch*	*Azure Monitor, Application*	*Google cloud monitoring*
Logging	*CloudWatch Logs, CloudTrail*	*Log Analytics, Security Event Logs*	*Cloud Logging*
Compliance	*CloudHSM*	*TrustCenter*	-

1. ***Identity and access management*** :
   Juga dikenal sebagai manajemen identitas dan akses, adalah kerangka kerja strategis dan teknologi untuk memastikan bahwa pengguna yang tepat memiliki akses yang tepat ke sumber daya teknologi. Sistem IDM adalah bagian dari kerangka kerja lengkap untuk manajemen data dan keamanan TI

   IAM : Adalah solusi untuk mengelola akses dan identitas pengguna dalam sumber daya *TI*. Solusi manajemen identitas dan akses mampu mengidentifikasi, mengautentikasi, dan memberikan hak akses yang sesuai kepada pengguna yang akan menggunakan sumber daya komputasi ini. Solusi ini dapat memastikan bahwa pengguna mengakses sumber daya *TI*

   Active Directory : Layanan direktori yang menyimpan konfigurasi jaringan untuk berbagai pengguna, grup, komputer, perangkat, dan kebijakan keamanan dalam database pusat. Peran *Active Directory* dalam jaringan seperti buku telepon yang menyimpan daftar alamat beserta informasi sensitif.

2. ***Key management*** : Manajemen kunci mengacu pada manajemen kunci kriptografi dalam sistem kriptografi. Ini termasuk pembuatan, pertukaran, penyimpanan, penggunaan, hashing, dan penggantian kunci. Ini termasuk desain protokol kriptografi, server backend, prosedur pengguna, dan protokol terkait lainnya.

   KMS *: AWS Key Management Service (KMS*) memungkinkan Anda membuat dan mengelola kunci kriptografik dengan mudah serta mengontrol penggunaan layanan dan aplikasi *AWS* Anda. *AWS KMS* adalah layanan tangguh dan aman yang menggunakan modul keamanan perangkat keras yang telah divalidasi ke FIPS 1402 atau sedang dalam proses divalidasi untuk melindungi kunci Anda.

   Azure Key Vault : adalah layanan cloud untuk menyimpan dan mengakses rahasia dengan aman. Rahasia adalah apa pun yang ingin Anda kontrol dengan ketat aksesnya, seperti kunci *API*, kata sandi, sertifikat, atau kunci kriptografi.

3. ***Network*** **:** adalah sekelompok komputer yang terhubung yang dapat berbagi sumber daya (seperti printer atau modem) dan data. Secara sederhana, suatu jaringan dapat menghubungkan setiap perangkat sehingga dapat saling berkomunikasi sehingga dapat mengirimkan informasi ke target

   VPC : *VPC* membantu Anda membuat lingkungan jaringan berbasis cloud yang terpisah, termasuk penyesuaian rentang alamat IP, segmen jaringan, tabel perutean, dan gateway. Selain itu, Anda dapat menghubungkan *VPC* dan *IDC* tradisional melalui *leased line, VPN*, atau *GRE* untuk menyediakan layanan *cloud hybrid.*

   VPN **(*Virtual Private Network*)**: Layanan koneksi yang menyediakan akses aman dan pribadi ke situs web dengan mengalihkan koneksi melalui server dan menyembunyikan komunikasi.

4. ***Security Check*** : Sistem yang dirancang untuk meningkatkan keamanan data, aplikasi, atau infrastruktur *TI* lainnya. Banyak aspek yang terkait langsung dengan keamanan cloud. Ini termasuk kontrol cloud, teknologi, dan kebijakan.

   Trusted Advisors : menyediakan rekomendasi yang membantu Anda mengikuti praktik terbaik *AWS. Trusted Advisor* mengevaluasi akun Anda menggunakan pemeriksaan. Pemeriksaan ini mengidentifikasi cara untuk mengoptimalkan infrastruktur

   Amazon Inspector : Penilaian Keamanan Otomatis membantu meningkatkan keamanan dan kepatuhan aplikasi yang diterapkan di *AWS. Amazon Inspector* secara otomatis menilai kerentanan, lubang keamanan, dan penyimpangan dari praktik terbaik aplikasi

   Security Center: Seseorang yang dapat menghubungkan informasi yang dikumpulkan dari berbagai solusi keamanan jaringan yang ada dan menganalisis insiden keamanan saat ini.

   CSPM : *Cloud Security Posture Management* Kesalahan konfigurasi keamanan adalah salah satu penyebab paling umum dari pelanggaran cloud. CSPM membantu menegakkan kebijakan keamanan perusahaan di cloud dan secara otomatis mengidentifikasi dan

memulihkan kesalahan konfigurasi yang menempatkan perusahaan dan datanya di ris

5. ***Storage Security*** : Sistem yang dirancang untuk meningkatkan keamanan data, aplikasi, atau infrastruktur komputasi lainnya. Ada beberapa aspek yang terkait langsung dengan keamanan cloud. Ini termasuk tata kelola cloud, teknologi, dan kebijakan

   Data Encryption for S3 : Sebagai algoritma kunci simetris, *DES* menggunakan kunci yang sama untuk mengenkripsi dan mendekripsi data. Jika algoritma yang digunakan adalah algoritma asimetris, gunakan kunci yang berbeda untuk enkripsi dan dekripsi.

   Storage Service Encryption : adalah program yang mengenkripsi pesan sehingga tidak dapat dibaca atau diketahui orang lain tanpa pengetahuan khusus. Atau yang dimaksud dengan enkripsi adalah proses "mengaburkan" informasi sehingga tidak dapat dibaca tanpa pengetahuan khusus.

   Access Control list : mengelompokkan paket berdasarkan kategori. Daftar akses bisa sangat berguna ketika Anda perlu mengontrol lalu lintas jaringan. daftar akses menjadi alat pilihan untuk pengambilan keputusan dalam situasi ini

6. ***Monitoring*** : Pemantauan adalah proses pengumpulan data yang dilakukan secara teratur dan mengukur kemajuan terhadap tujuan program. Pemantauan bertujuan untuk melacak perubahan dan fokus pada proses dan hasil

   Cloud Watch : CloudWatch adalah layanan untuk memantau sumber daya cloud AWS dan aplikasi yang berjalan di AWS. Anda dapat menggunakan Amazon CloudWatch untuk mengumpulkan dan melacak metrik, mengumpulkan dan melacak file log, serta menyetel alarm.

   Windows Azure : Ini dapat digunakan untuk membangun, mengembangkan, dan menjalankan aplikasi web yang berjalan di pusat data *Microsoft. Windows Azure* menyediakan beberapa jenis layanan utama, termasuk: Situs web *(hosting web*)

   ***Google Cloud Monitoring*:** Adalah layanan cloud publik yang menyediakan berbagai layanan seperti komputasi, penyimpanan, data besar, pembelajaran mesin (ML), pengembangan aplikasi, dan banyak lagi. Seperti aplikasi berbasis cloud lainnya, *Google Cloud* memerlukan pemantauan konstan untuk menjaga kesehatan dan performa secara keseluruhan.

7. ***Logging*** : Menerima entri log melalui *Cloud Logging API* tempat entri tersebut melewati *log router*. *Router log* memeriksa setiap entri log terhadap filter penyertaan dan pengecualian yang ada untuk menentukan entri log mana yang harus dihapus, mana yang harus diimpor, dan mana yang harus disertakan dalam output.

   Cloud Watch : *CloudWatch* adalah layanan untuk memantau sumber daya *cloud AWS* dan aplikasi yang berjalan di *AWS*. Anda dapat menggunakan Amazon *CloudWatch* untuk mengumpulkan dan melacak metrik, mengumpulkan dan melacak file log, serta menyetel alarm.

   CloudTrail : yang sangat informatif di lingkungan *AWS* Anda. Selain itu, tim dapat menggunakannya untuk melakukan deteksi anomali dasar dengan menambahkan status. Dalam pembicaraan ini, *Travis McPeak* dan *Will Bengtson* dari *Netflix* memamerkan sistem yang dibangun secara ketat dengan komponen *AWS* berpemilik yang memantau aktivitas *CloudTrail* di lingkungan multi-akun dan mengirim peringatan saat aplikasi sedang berjalan. digunakan untuk melakukan tindakan yang tidak wajar

   Log Analytics : Platform logging dan data beban kerja yang diimpor ke *Cloud Logging* tersedia di *Log Analytics*, yang didukung oleh *BigQuery*. Lakukan analisis lanjutan menggunakan *SQL* untuk mengkueri log Anda. Data log juga tersedia langsung di *BigQuery* sehingga Anda dapat menautkan log ke data bisnis lainnya.

   ***Cloud Logging*`**: Menerima entri log melalui *API* tempat entri tersebut melewati *router log. Router log* memeriksa setiap entri log terhadap filter penyertaan dan pengecualian yang ada untuk menentukan entri log mana yang harus dihapus, mana yang harus diimpor, dan mana yang harus disertakan dalam output.

8. ***Cloud compliance*** : Adalah prinsip bahwa sistem yang dikirimkan di cloud harus memenuhi standar yang disyaratkan oleh pelanggan. Cloud compliance memastikan

layanan cloud memenuhi persyaratan dan kebutuhan

Cloud HSM : Kunci enkripsi dapat dilindungi dalam *HSM* yang dirancang dan disetujui menurut standar pemerintah untuk manajemen kunci yang aman. Anda dapat membuat, menyimpan, dan mengelola kunci enkripsi yang digunakan untuk mengenkripsi data Anda dengan aman, sehingga hanya Anda yang dapat mengaksesnya.

Trust Center : Melindungi komputer Anda dari serangan dan melindungi informasi pribadi di komputer Anda telah menjadi tantangan yang lebih besar ketika menghubungkan ke infrastruktur Internet yang tidak tepercaya kepercayaan telah menjadi populer.

Kesimpulan

Penelitian ini menjelaskan bagaimana tiga layanan komputasi awan memberikan solusi untuk keamanan. Perbedaan produk yang ditawarkan oleh ketiga layanan tersebut serta perbandingan yang dijelaskan dan dilampirkan pada penelitian ini dapat memudahkan konsumen untuk memilih merek yang tepat sehingga Dengan bantuan penelitian ini dapat menghindari kerugian yang ditimbulkan oleh konsumen karena ketidakpahaman terhadap spesifikasi yang dipilih oleh konsumen.

DAFTAR PUSTAKA

-. (2019). *Arsitektur Keamanan: Apa dan Bagaimana?* https://manajemen-ti.com/arsitektur-keamanan-apa-dan-bagaimana/

-. (2021). *Indeks Keamanan Siber Indonesia Kalah dari Malaysia-Filipina*. CNN INDONESIA. https://www.cnnindonesia.com/teknologi/20210905084610-185-689865/indeks-keamanan-siber-indonesia-kalah-dari-malaysia-filipina

Anuj Varma. (2020). *Security Audits of AWS Accounts – Roles, Policies and equivalents on GCP and Azure*. January 20, 2020. https://www.anujvarma.com/security-audits-of-aws-accounts-what-roles-and-policies-do-i-need/

byDale. (2012). *Top 13 Network Security Features*. 12.05.12. https://www.plixer.com/blog/top-13-network-security-features/

Citradi, T. (2020). *Data Pengguna E-Commerce Bocor, Ini Bukti RI Rawan Cybercrime*. CNBC INDONESIA. https://www.cnbcindonesia.com/tech/20200706140435-37-170521/data-pengguna-e-commerce-bocor-ini-bukti-ri-rawan-cybercrime

G, F. M., Saedudin, R. R., Almaarif, A., Kom, S., Prodi, S., Informasi, S., Industri, F. R., & Telkom, U. (2020). *Analisis Performansi Metrik CPU Dan Memory Pada Windows Azure Virtual Machine (VM) dan Amazon Web Service Elastic Compute Cloud (EC2)*. *7*(2), 6975–6983.

Hakim, A. R. (2016). Analisis Perbandingan Sistem Cloud Azure Dan Google Cloud. *InfoTekJar (Jurnal Nasional Informatika Dan Teknologi Jaringan)*, *1*(1), 38–41. https://doi.org/10.30743/infotekjar.v1i1.38

MyBlockchainExperts. (2019). *Top 10 Google Cloud Platform (GCP) Security Best Practices*. November 1, 2019. https://myblockchainexperts.org/2019/11/01/top-10-google-cloud-platform-gcp-security-best-practices/

Riley, C. (2017). *AWS Security vs. Azure Security*. September 27, 2017. https://www.sumologic.com/blog/aws-security-vs-azure-security/

Wankhede, P., Talati, M., & Chinchamalatpure, R. (2020). Comparative Study of Cloud Platforms - Microsoft Azure, Google Cloud Platform and Amazon Ec2. *Journal of Research in Engineering and Applied Sciences*, *05*(02), 60–64. https://doi.org/10.46565/jreas.2020.v05i02.004

Wardani, A. setyo. (2020). *https://www.liputan6.com/tekno/read/4469008/pengguna-internet-dunia-tembus-466-miliar-rata-rata-online-di-smartphone*. Liputan 6. https://www.liputan6.com/tekno/read/4469008/pengguna-internet-dunia-tembus-466-miliar-rata-rata-online-di-smartphone (Anuj Varma, 2020; byDale, 2012; MyBlockchainExperts, 2019; Riley, 2017)

Cynthia Harvey. (2021). *AWS vs. Azure vs. Google Cloud: 2021 Cloud Platform Comparison*. 14 Agustus 2021. https://www.datamation.com/cloud/aws-vs-azure-vs-google-cloud/

Shanika Wickramasinghe. (2021). *AWS vs Azure vs GCP: Comparing The Big 3 Cloud Platforms*. 1 Oktober. https://www.bmc.com/blogs/aws-vs-azure-vs-google-cloud-platforms/

John Emmitt. (2021). *Aws vs, azure vs, google Cloud: Comparing cloud platfroms*. 13 Mei. https://www.kaseya.com/blog/2021/05/13/aws-vs-azure-vs-google-cloud/

TRIPWIRE GUEST AUTHORS. (2019). *AWS vs. Azure vs. Google – What's the Difference from a Cloud Security Standpoint*. 29 Desember. https://www.tripwire.com/state-of-security/security-data-protection/cloud/aws-azure-google-difference-cloud-security-standpoint/

Tom Allen. (2020). *Microsoft vs Google vs AWS: Which cloud giant leads identity and access management*. 23 September. https://www.computingdelta.com/2020/09/23/microsoft-vs-google-vs-aws-which-cloud-giant-leads-iam/

Jimmy Idemudia. (2021). *The Best IAM Services Comparison: Google Cloud Vs. AWS Vs. Azure*. 28 October. https://rivalime.com/iam-services-comparison/

Priya Pedamkar. (n.d.). *AWS vs Azure vs Google Cloud*. `. https://www.educba.com/aws-vs-azure-vs-google-cloud/

MEENAKSHI KASI. (2021). *AWS vs. Azure vs. Google Cloud: Choosing the Best Cloud Platform*. 11 Februari. https://www.varonis.com/blog/aws-vs-azure-vs-google/

G, F. M., , Rd. Rohmat Saedudin, S.T, M., & , Ahmad Almaarif, S.Kom, M. (n.d.). *ANALISIS PERFORMANSI METRIK CPU DAN MEMORY PADA WINDOWS AZURE VIRTUAL MACHINE (VM) DAN AMAZON WEB SERVICE ELASTIC COMPUTE CLOUD (EC2)*.

byDale. (2012). *Top 13 Network Security Features*. 12.05.12. https://www.plixer.com/blog/top-13-network-security-features/

MyBlockchainExperts. (2019). *Top 10 Google Cloud Platform (GCP) Security Best Practices*. November 1, 2019. https://myblockchainexperts.org/2019/11/01/top-10-google-cloud-platform-gcp-security-best-practices/

Riley, C. (2017). *AWS Security vs. Azure Security*. September 27, 2017. https://www.sumologic.com/blog/aws-security-vs-azure-security/

Anuj Varma. (2020). *Security Audits of AWS Accounts – Roles, Policies and equivalents on GCP and Azure*. January 20, 2020. https://www.anujvarma.com/security-audits-of-aws-accounts-what-roles-and-policies-do-i-need/

View publication stats